修 士 論 文 の 和 文 要 旨

研究科・専攻	大学院　　電気通信学研究科　　情報工学専攻　博士前期課程		
氏　　名	神山 貴幸	学籍番号	0731012
論 文 題 目	コールスタック情報を利用したモデル分割に基づく異常検知システム		

要　　旨

アプリケーションの脆弱性を突く攻撃を防止するために，正常な実行におけるシステムコールのパターンを用いた異常検知システムが数多く提案されてきた．しかし，それらの多くはプログラム全体で，一つの大きな正常動作のモデルを作成しているため，プログラムの異なるフェーズにおけるシステムコール呼び出しの情報が融合され，検知精度が下がるという問題がある．このような問題を解決するため，本研究では，モデル分割に基づく異常検知システム PhaIDS を提案する．このシステムは，実行時のコールスタックの情報を用いて，プログラムの実行をフェーズに自動的に分割し，フェーズ毎に正常動作のモデルを作成する．また，プログラムの実行状態に応じて，正常動作のモデルを動的に切り替えることで，実行状態に応じた異常検知を実現する．PhaIDS は Linux 上に実装し，システムの有効性を検証するために，生成されるモデルの分割数と検知精度，PhaIDS 導入によるオーバヘッド，既存手法の検知の回避を狙った攻撃を検知できるかどうかについて実験を行い，既存手法との比較を行った．その結果，PhaIDS によって生成されるモデルが，既存手法より検知を回避されにくいモデルとなっていることを確認した．